National Infrastructure Protection Center
CyberNotes

Issue #2002-06 *March 25, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 7 and March 22, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Apache Group[1]	Windows 95/98/NT 4.0/2000, XP	Apache 1.3.6win32, 1.3.9win32, 1.3.11win32 -1.3.20 win32; 1.3.22win32, 1.3.23win32, 2.0.28-BETA win32, 2.0.32-BETA win32	A vulnerability exists due to the way DOS batch scripts are handled by the Apache web server, which could let a remote malicious user execute arbitrary commands.	This issue has been addressed in Apache 1.3.24 and 2.0.34-BETA for Microsoft Windows operating systems. Administrators are advised to upgrade as soon as these fixed versions become available.	Apache Win32 Batch File Command CVE Name: CAN-2002-0061	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[1] Bugtraq, March 21, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
ARSC Really Simple Chat[2]	Multiple	ARSC Really Simple Chat 1.0, 1.0.1	A Path Disclosure vulnerability exists when a request is made for a non-existent page, which could let a remote malicious user obtain sensitive information.	Patch available at: http://manuel.kiessling.net/projects/software/arsc/download/arsc1.0.1p1.zip	ARSC Really Simple Chat Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
AT&T[3]	Unix	VNC 3.3.3R2	A Denial of Service vulnerability exists in the RedHat Virtual Network Computing (VNC) HTTP server implementation.	Upgrade available at: ftp://updates.redhat.com/	VNC HTTP Server Denial of Service	Low	Bug discussed in newsgroups and websites.
Avaya Labs[4]	Unix	Libsafe 2.0-9-2.0-11	Several Format String vulnerabilities exist due to incorrect parsing and lack of implementation of some format specified types, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.research.avayalabs.com/project/libsafe/src/libsafe-2.0-12.tgz	Libsafe Format String	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
BG Guestbook[5]	Multiple	BG Guestbook 1.0	A Cross-Site Scripting vulnerability exists in some of the input fields on the posting form, which could let a remote malicious user execute arbitrary script code.	Upgrade available at: http://billyg.no-ip.com:8080/bggb/download.php	BG Guestbook Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
Big Sam[6]	Multiple	Big Sam 1.1.08	A vulnerability exists when a large parameter is passed to the script, which could let a malicious user obtain sensitive information.	Upgrade available at: http://zadrozynski.free.fr/bigsam/bigsam.1_1_09.php.txt	Big Sam Sensitive Information	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
BitVise[7]	Windows NT 4.0/2000, XP	WinSSHD 1.1	A Denial of Service vulnerability exists due to "ill-intended connection attempts."	Upgrade available at: http://www.bitvise.com/existing-users.html	WinSSHD Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Black Tie Project[8]	Multiple	Black Tie Project 0.5b	A Path Disclosure vulnerability exists when a request is made for a non-existent page, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Black Tie Project Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Caldera[9]	Unix	SCO Open Server 5.0.5, 5.0.6	A buffer overflow vulnerability exists in the 'dlvr_audit' command, which could let a malicious user obtain root access.	Upgrade available at: ftp://ftp.caldera.com/pub/openserver5/oss645a	OpenServer dlv_audit Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[2] ALPER Research Labs Security Advisory, ARL02-A07, March 16, 2002.
[3] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:026-43, March 21, 2002.
[4] Bugtraq, March 18, 2002.
[5] ALPER Research Labs Security Advisory, ARL02-A08, March 16, 2002.
[6] ALPER Research Labs Security Advisory, ARL02-A11, March 17, 2002.
[7] KPMG-2002005, March 18, 2002.
[8] ALPER Research Labs Security Advisory, ARL02-A06, March 12, 2002.
[9] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.8, March 11, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Caupo.net[10]	Multiple	CaupoShop 1.30rc4, 1.30a	A Cross-Site Scripting vulnerability exists due to inadequate checking for malicious code when a new customer registers, which could let a malicious user execute arbitrary script code.	Update available at: http://www.caupo.com/soft/download/CaupoShop-Classic-130-rc4.zip	CaupoShop Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Check Point Software Technol-ogies[11]	Multiple	Firewall-1 4.0, 4.0SP1-8, 4.1, 4.1SP1-5; Next Generation 0.0; VPN-1 4.1, 4.1SP1-4	A vulnerability exists when 'SecuRemote' or 'SecuClient' are used for authentication, which could let a remote malicious user by pass security restrictions.	No workaround or patch available at time of publishing.	FW-1 SecuClient/ SecuRemote Security Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Christof Pohl[12, 13]	Unix	Improved mod_front page 1.3.1, 1.3.2, 1.4.1, 1.5, 1.5.1	A buffer overflow vulnerability exists due to the lack of boundary checks in 'fpexec.c,' which could let a remote malicious user execute arbitrary code with superuser privileges.	**Mandrake:** ftp://download.sourceforge.net/pub/mirrors/mandrake/updates/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/www/	Improved mod_frontpage Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Citadel/UX [14]	Unix	Citadel/UX 5.90	A Denial of Service vulnerability exists due to a buffer overflow in the 'HELO' command.	No workaround or patch available at time of publishing.	Citadel/UX Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Claymore Systems, Inc.[15]	Multiple	PureTLS 0.9b1	A vulnerability exists which could let a remote malicious user eavesdrop on or take over a protected communication session.	Upgrade available at: http://www.rtfm.com/cgi-bin/distrib.cgi?puretls-0.9b2.tar.gz	PureTLS Injection Attack	Medium	Bug discussed in newsgroups and websites.
Dave Lawrence[16]	Unix	XTux 2001.06.01	A Denial of Service vulnerability exists when unexpected characters are sent to the server.	No workaround or patch available at time of publishing.	XTux Server Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[10] Securiteam, March 16, 2002.
[11] Bugtraq, March 8, 2002.
[12] Mandrake Linux Security Update Advisory, MDKSA-2002:021, March 7, 2002.
[13] FreeBSD Security Advisory, FreeBSD-SA-02:17, March 12, 2002.
[14] Bugtraq, March 9, 2002.
[15] Securiteam, March 9, 2002.
[16] Bugtraq, March 9, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Ecartis/ Listar[17]	Unix	Ecartis Ecartis 1.0.0 snapshot 20020125, 20020121; Listar Listar 0.126a, 0.127a, 0.129a	Multiple buffer overflow vulnerabilities exist as well as an improper privilege dropping vulnerability, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Ecartis/Listar Multiple Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Foundry Networks[18]	Multiple	EdgeIron 4802F 0.0	A vulnerability exists in the default SNMP configuration, which could let a remote malicious user overwrite and read sensitive information.	Use the access control list feature built into the switch: EdgeIron(config)# EdgeIron(config)#snmp-server security EdgeIron(config)# EdgeIron(config)#snmp-server user <name> <community-string> <ip-address>	EdgeIron SNMP Configuration Sensitive Information	Medium	Bug discussed in newsgroups and websites. This vulnerability may be exploited with a SNMP client.
Foundry Networks[19]	Multiple	ServerIron 5.1.10t12, 6.0, 7.1.09, ServerIron400 0.0, ServerIron800 0.0, ServerIron XL 0.0, XL/G 0.0	A vulnerability exists because URLs are not correctly decoded, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ServerIron URL Decode	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Francisco Burzi[20]	Unix	PHP-Nuke 5.0-5.4	A vulnerability exists when a maliciously constructed HTTP request is sent to the 'index.php' script, which could let al malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP-Nuke Path Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Francisco Burzi[21]	Unix	PHP-Nuke 5.0-5.4, PostNuke 0.62-0.64, 0.7, 0.70	A vulnerability exists when if a malicious cookie is sent, which could let a malicious user hijack arbitrary user accounts including those with administrative privileges.	Upgrade available at: http://www.postnuke.com/modules.php?op=modload&name=Downloads&file=index&req=getit&lid=169	PHP-Nuke Account Hijacking	Medium/ **High** **(High if adminis-trative privileges are obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.
GNU[22]	Unix	Fileutils 4.0, 4.1, 4.1.6	A race condition vulnerability exists in various utilities, which could let a malicious user delete the whole file system.	Patch available for 4.1.6 at: http://mail.gnu.org/pipermail/bug-fileutils/2002-March/002440.html	Fileutils Race Condition	Medium	Bug discussed in newsgroups and websites.

[17] Securiteam, March 15, 2002.
[18] Securiteam, March 22, 2002.
[19] Securiteam, March 16, 2002.
[20] Bugtraq, March 20, 2002.
[21] Bugtraq, March 17, 2002.
[22] Securiteam, March 15, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Hosting Controller[23]	Windows NT 4.0/2000	Hosting Controller 1.4, 1.4.1	Several Directory Traversal vulnerabilities exist because user privileges are not validated, which could let a malicious user modify, delete, or create files and directories outside of the web root.	No workaround or patch available at time of publishing.	Hosting Controller Weak Permissions Checking	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Imlib[24]	Unix	Imlib 1.9-1.9.12	Two vulnerabilities exist; a vulnerability exists because malformed image files can be loaded, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code; and a vulnerability exists in the 'NetPBM' library, which could let a malicious user execute an untrusted image.	Patch available at: ftp://updates.redhat.com/	Imlib Untrusted Images	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
IncrediMail Ltd.[25]	Windows 95/98/ME/ NT 4.0/2000, XP	IncrediMail 0.0 Build 618, Build 560, Build 1400185	A vulnerability exists when an e-mail is received that includes a file attachment because the file is automatically stored in a predictable location, which could let a remote malicious user execute arbitrary programs.	No workaround or patch available at time of publishing.	IncrediMail Attachment Location	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Internet Security Systems[26]	Multiple	RealSecure for Nokia 6.0	A vulnerability exists in the 'ISS.ACCESS' configuration file, which could let a malicious user gain control of the NIDS daemon and its components.	Upgrade available at: http://www.nokia.com/securenetworksolutions/trnsup/index.html	RealSecure for Nokia Default Configuration	**High**	Bug discussed in newsgroups and websites.
Jerrett Taylor[27]	Multiple	PHP ImgList 1.1, 1.2, 1.2.1	A Directory Traversal vulnerability exists when a specially crafted HTTP request is sent, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.liquidpulse.net/get.lp?id=17	PHP ImgList Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
John Roy[28]	Windows 95/98/NT 4.0/2000	Pi3Web 1.0.1, 1.0.3, Pi3Web for Windows 2.0.0	A vulnerability exists in the default configuration when a non-existent page is requested, which cold let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Pi3Web Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Linksys[29]	Multiple	EtherFast BEFVP41 Router 0.0	A vulnerability exists when a 3DES key and MD5 authentication key are entered because the keys are truncated, which could result in weaker than expected encryption.	No workaround or patch available at time of publishing.	EtherFast BEFVP41 Key Weak Encryption	Medium	Bug discussed in newsgroups and websites.

[23] Bugtraq, March 18, 2002.
[24] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:048-06, March 20, 2002.
[25] Bugtraq, March 15, 2002.
[26] NMRC Nomad Mobile Research Centre Advisory, March 20, 2002.
[27] Securiteam, March 16, 2002.
[28] Bugtraq, March 10, 2002.
[29] Bugtraq, March 8, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Linux Directory [30]	Unix	Penguin Traceroute 1.0	A vulnerability exists because special characters are not adequately filtered, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Penguin Traceroute Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites.
Linux-Sottises[31]	Unix	Board-TNK 1.3, News-TNK 1.2.1	A Cross-Site Scripting vulnerability exists because input is not properly filtered, which could let a malicious user execute arbitrary script code.	**Linux-Sottises news-tnk 1.2.1:** http://www.linux-sottises.net/software/news-tnk_v1.2.2.tar.gz **Linux-Sottises board-tnk 1.3:** http://www.linux-sottises.net/software/board-tnk_v1.3.1.tar.gz	Board-TNK & News-TNK Cross Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Macro-media[32]	Windows 95/98/ME/ NT 4.0/2000, XP	Macromedia Flash 5.0	A vulnerability exists in the FSCommand 'save' and 'exec' commands, which could let a remote malicious user execute arbitrary code.	Patch available at: http://download.macromedia.com/pub/flashplayer/updaters/5/flashplayer_updater.zip	Macromedia Flash Undocumented Command & Undocument File Access	**High**	Bug discussed in newsgroups and websites.
Marcus S. Xenakis[33]	Unix	Directory. php 0.0	A vulnerability exists in the 'directory.php' script, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Directory.php Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
MenaSoft[34]	Windows 95/98/NT 4.0/2000, Unix	SPHER Eserver 0.99I, 0.99f	A Denial of Service vulnerability exists when multiple connections are made to the server from a single machine.	No workaround or patch available at time of publishing.	SPHEREserver Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft [35] ***Microsoft re-releases bulletin[36]***	**Windows 2000, XP**	**Exchange Server 2000 0.0, 2000 0.0 SP1&2, Advanced Server 0.0. 0.0 SP1&2, Professional 0.0, 0.0SP1&2, 2000 Server 0.0, 0.0SP1&2, XP Professional 0.0**	**A remote Denial of Service vulnerability exists when certain types of malformed SMTP commands are sent to the server.** ***Updated bulletin issued states that the Windows 2000 patch for MS02-012 and MS02-011 are the same.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-012.asp**	**Microsoft SMTP Service Malformed Data Remote Denial of Service** **CVE Name: CAN-2002-0055**	**Low**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[30] Securiteam, March 22, 2002.
[31] ALPER Research Labs Security Advisory, ARL02-A09, Match 15, 2002.
[32] Bugtraq, March 19, 2002.
[33] Itcp Advisory 3, March 10, 2002.
[34] ISS Security Alert Summary, AS02-10, March 11, 2002.
[35] Microsoft Security Bulletin, MS02-012, February 27, 2002.
[36] Microsoft Security Bulletin, MS02-012 (Version 2.0), March 12, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft [37] *Microsoft re-releases bulletin*[38]	Windows 95/98/ME/ NT 4.0/2000, XP	All builds of the Microsoft VM up to and including build 3802	A session hijacking vulnerability exists due to the way Java requests for proxy services are handled, which could let a remote malicious user take any action or combination of actions of his/her choosing. *A second vulnerability exists that is a variant of the "Virtual Machine Verifier" vulnerability discussed in MS99-045. A flaw exists in the security checks on casting operations within the Microsoft VM, which could let a malicious user execute arbitrary code.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-013.asp *Customers who have previously installed the new build do not need to take any additional action.*	Microsoft Java Applet Browser Traffic Redirect CVE Names: CAN-2002-0058; *CAN-2002-0076*	High	Bug discussed in newsgroups and websites. *Vulnerability has appeared in the press and other public media.*
Microsoft [39] *Microsoft re-releases bulletin*[40]	Windows NT 4.0/2000	Exchange Server 5.5, 5.5SP1-4, 2000 Advanced Server 0.0, 0.0SP1&2, Datacenter Server 0.0, 0.0SP1&2, Professional 0.0, 0.0SP1&2, 2000 Server 0.0, 0.0SP1&2	A vulnerability exists in the way that the Windows 2000 SMTP service and Microsoft Exchange Server 5.5 interact with the NTLM authentication layer, which could let a malicious user obtain unauthorized user-level access to the SMTP service. *Updated bulletin issued states that the Windows 2000 patch for MS02-012 and MS02-011 are the same.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-011.asp	Microsoft Windows SMTP Service Authenti-cation CVE Name: CAN-2002-0054	Medium	Bug discussed in newsgroups and websites.
Microsoft [41] *Microsoft re-releases bulletin*[42]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.01, 5.01SP1&2, 5.5, 5.5SP1&2, 6.0	A vulnerability exists in the way VBScript is handled in IE relating to validating cross-domain access, which could let a malicious user obtain sensitive information. *Updated bulletin released stating since the release of the original patch, Microsoft has become aware that some third-party scripting languages may be affected by this vulnerability.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-009.asp *Customers who experience problems with third-party applications after applying the original patch should download the revised patch.*	Internet Explorer VBScript Policy Violation CVE Name: CAN-2002-0052	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[37] Microsoft Security Bulletin, MS02-013, March 4, 2002.
[38] Microsoft Security Bulletin, MS02-013 (Version 2.0), March 18, 2002.
[39] Microsoft Security Bulletin, MS02-011, February 27, 2002.
[40] Microsoft Security Bulletin, MS02-011 (Version 2.0), March 12, 2002.
[41] Microsoft Security Bulletin, MS02-009, February 21, 2002.
[42] Microsoft Security Bulletin, MS02-009 (Version 1.1), March 13, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft[43]	Windows 95/98/ME/ NT 4.0/2000	Outlook 2002 0.0, Outlook Express 6.0	Multiple vulnerabilities exist: a vulnerability exists when a Windows Media Player file is referenced in an IFRAME tag, which could let a malicious user execute arbitrary JavaScript commands; a vulnerability exists because cookies can be set and read even when the default settings claim that cookies are turned off; a vulnerability exists because JavaScript code can still be executed in spite of the fact that scripting is turned off by default; and a vulnerability exists if a user simply reads an HTML email message containing a URL embedded in the IFrame tag, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Outlook Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the Cookie Bypass vulnerability and IFrame vulnerability. Vulnerabilities have appeared in the press and other public media.
Microsoft[44] ***New versions of bulletin released***[45, 46, 47]	**Windows 95/98/NT 4.0/2000, XP**	**Windows 95, 98, 98SE, NT 4.0, NT 4.0 Server, Terminal Server Edition, 2000, XP**	**A buffer overflow vulnerability exists because the component of the SNMP agent service that parses incoming commands contains an unchecked buffer, which could let a malicious user cause a Denial of Service or execute arbitrary code.** ***On March 11, Microsoft released an updated version of the bulletin announcing the availability of a patch for Windows NT 4.0 Terminal Server Edition and to advise customers that the work-around procedure is no longer needed for that platform. On March 14, 2002, Microsoft discovered that the English and German patches for Windows NT 4.0 Terminal Server Edition contained incorrect files.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-006.asp** ***It is recommended that customers who have downloaded the Windows NT 4.0 Terminal Server Edition patch in English or German prior to March 14, 2002 install the updated version. Customers who have installed the Windows NT 4.0 Terminal Server Edition patches in any language other than English or German do not need to take any action.***	**Windows Unchecked Buffer SNMP Service** **CVE Name: CAN-2002-0053**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**

[43] Bugtraq, March 20, 2002.
[44] Microsoft Security Bulletin, MS02-006, February 15, 2002.
[45] Microsoft Security Bulletin, MS02-006 (version 3.0), March 5, 2002.
[46] Microsoft Security Bulletin MS02-006 (version 4.0), March 11, 2002.
[47] Microsoft Security Bulletin MS02-006 (version 5.0), March 14, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Microsoft[48]	Windows NT 4.0/2000	Windows NT Workstation 4.0, 4.0SP1-6a; Terminal Server 4.0, 4.0SP1-6a; Server 4.0, 4.0SP1-6a; Enterprise Server 4.0, 4.0SP1-6a; 000 Terminal Services 0.0, 0.0SP1-2; 2000 Server 0.0, 0.0SP1-2; 2000 Professional 0.0, 0.0SP1-2; 2000 Datacenter Server 0.0, 0.0SP1-2; 2000 Advanced Server 0.0, 0.0SP1-2	A vulnerability exists in the debugging subsystem, which could let a malicious user execute arbitrary code with SYSTEM privileges.	No workaround or patch available at time of publishing.	Windows 2000/NT 4.0 Privilege Elevation	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[49]	Windows NT 4.0	Microsoft Windows NT Server 4.0, 4.0 SP1-6a	A vulnerability exists in a number of .HTR files due to the way change password requests are handled, which could let a remote malicious user bypass the administrator security policy to change their password.	No workaround or patch available at time of publishing.	Windows NT Password Changing Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[50]	Windows 95/98/ME/ NT 4.0/2000, XP	MSN Messenger Service 3.6	A vulnerability exists which could let a malicious user send messages through the server that appear to have originated from an arbitrary user.	No workaround or patch available at time of publishing.	MSN Messenger Message Spoofing	Medium	Bug discussed in newsgroups and websites.

[48] NTBugtraq, March 14, 2002.
[49] Securiteam, March 9, 2002.
[50] Bugtraq, March 19, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Multiple Vendors[51]	Windows 95/98/ME/ NT 40/2000, XP; MacOS 9.0-9.2.2, MacOS X 10.0-10.1.2	Microsoft Internet Explorer 5.01, 5.01SP1&2, 5.5. 5.5SP1&2, 6.0; Mozilla Browser 0.8-0.9.8; Opera Software Opera Web Browser 5.02 win32, 5.10-5.12, 6.0.1win32	A Denial of Service vulnerability exists due to a flaw in the JavaScript interpreter.	No workaround or patch available at time of publishing.	Multiple Vendor JavaScript Interpreter Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[52, 53]	Unix	HP Java Web Start 1.0.00, 1.0.1.00; Sun Java Web Start 1.0, 1.0.1_01, 1.0.1	A vulnerability exists due to the way the Java Web Start is used to open unsigned applications, which could let an unauthorized malicious user obtain access to restricted resources.	**Hewlett Packard:** http://www.hp.com/products1/unix/java/java2/webstart/downloads/license_webstart_1-0-1-01.html **Sun MicroSystems:** Java Web Start 1.0.1_02: http://java.sun.com/products/javawebstart/index.html Java 2 SDK, v 1.4: http://java.sun.com/j2se/1.4/	Multiple Vendor Java Web Start Unsigned Application	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[54]	Unix	Linux kernel 2.4-2.4.18	A vulnerability exists in the UDP implementation that allows both active and passive fingerprinting of Linux machines, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Linux UDP Fingerprinting	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[51] Bugtraq, March 18, 2002.
[52] Sun Microsystems, Inc. Security Bulletin, #00217, March 18, 2002.
[53] Hewlett-Packard Company Security Bulletin, HPSBUX0203-188, March 19, 2002.
[54] Bugtraq, March 19, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Multiple Vendors[55, 56, 57, 58, 59, 60, 61, 62, 63,	Unix	ZLib 1.0-1.0.9, 1.1-1.1.3	A vulnerability exists in the decompression algorithm used by the compression library, which could let a malicious user conduct a Denial of Service attack, obtain sensitive information, or execute arbitrary code.	**Zlib:** http://www.gzip.org/zlib/ **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse **EnGarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **Debian:** http://security.debian.org/dists/stable/updates/main/ **Mandrake Linux:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp://ftp.openpkg.org/release/1.0/UPD/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:18/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/	ZLib Compression Library CVE Name: CAN-2002-0059	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[55] Red Hat Security Advisory, RHSA-2002:027-22, 2002:026-35 & 39, March 11, 2002.
[56] SuSE Security Announcement, SuSE-SA:2002:010 & 20002:011, March 11, 2002.
[57] EnGarde Secure Linux Security Advisory, ESA-20020311-008, March 11, 2002.
[58] Debian Security Advisory, DSA 122-1, March 11, 2002.
[59] Mandrake Linux Security Update Advisory, MDKSA-2002:022 & MDKSA-2002:023-1, March 12, 2002.
[60] OpenPKG Security Advisory, OpenPKG-SA-2002.003, March 12, 2002.
[61] Conectiva Linux Security Announcement, CLA-2002:469, March 14, 2002.
[62] FreeBSD Security Advisory, FreeBSD-SA-02:18, March 18, 2002.
[63] Trustix Secure Linux Security Advisory, TSLSA-2002-0040, March 18, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Multiple Vendors[64, 65]	Unix	HP Java JRE /JDK HP-UX 1.1.8, 1.2.2, 1.3; Sun JDK (Solaris Production Release) 1.1.8_14, 1.1.8_008, JDK (Windows Production Release) 1.1.8_008, JRE (Linux Production Release) 1.2.2_010, 1.3_05, (Solaris Production Release) 1.1.8_14, 1.2.2_10, 1.3_05, 1.3.1_01, 1.1.8_008, 1.2.2_10, (Windows Production Release) 1.1.8_008, 1.2.2_010, 1.3_05, 1.3.1_01a, SDK (Linux Production Release) 1.2.2_010, 1.3_05, 1.3.1_01, (Solaris Production Release) 1.2.2_10, 1.3_05, 1.3.1_01, 1.2.2_010, (Windows Production Release) 1.2.2_10, 1.3_05, 1.3.1_01a	A vulnerability exists due to a data casting error, which could let a malicious user execute arbitrary code. *NOTE: This vulnerability also exists in Microsoft and is explained under a Microsoft entry.*	**Hewlett Packard:** http://www.hp.com/products1/unix/java/ **Microsoft:** http://download.microsoft.com/download/vm/Install/3805/W9XNT4MeXP/EN-US/msjavx86.exe **Sun Microsystems:** http://java.sun.com/j2se/	Multiple Vendor Java Virtual Machine Bytecode Verifier CVE Name: CAN-2002-0076	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[64] Sun Microsystems, Inc. Security Bulletin, Sun-00218, March 18, 2002.
[65] Hewlett-Packard Company Security Bulletin, HPSBUX0203-187, March 19, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Oblix[66]	Windows NT 4.0/2000, Unix	NetPoint 5.2	A vulnerability exists because the account lockout policy can be bypassed, which could make the account vulnerable to automated or manual password cracking.	Oblix has released a patch which rectifies this issue. Contact Oblix Customer Support support@oblix.com	NetPoint Account Lock Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenBSD[67]	Unix	OpenBSD 3.0	Vulnerabilities exist in some of the userland utilities due to authentication process, which could let a malicious user obtain unauthorized access.	Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.0/common/016_approval.patch	OpenBSD Authentication	Medium	Bug discussed in newsgroups and websites.
Openwall Project[68]	Unix	Linux kernel 2.4.18 x86	A vulnerability exists because user privileges are disregarded when IPC signals are handled, which could let a malicious user kill processes not belonging to them.	**Openwall Project:** http://www.openwall.com/linux/linux-2.2.20-ow2.tar.gz	Linux kernel IPC Signal Handling	Medium	Bug discussed in newsgroups and websites.
Oracle Corporation[69]	Windows NT 4.0/2000, Unix	Oracle 9i Application Server 0.0	A vulnerability exists because user accounts are created during installation that have well-known default passwords, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Oracle Default Passwords	**Medium**	Bug discussed in newsgroups and websites. There is no exploit code required.
Oracle Corporation[70]	Windows NT 4.0/2000, Unix	Oracle 9i Application Server 0.0	A vulnerability exists in the 'OWA_UTIL PL/SQL' application due to the way procedures are stored, which could let a malicious user obtain sensitive information.	**Workaround available at:** http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf	Oracle 9iAS PL/SQL OWA_UTIL Procedure Exposure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Oracle Corporation[71]	Multiple	Oracle 9i Application Server 1.0.2, Oracle8i 8.1.7, 8.1.7.1, Oracle9i 9.0, 9.0.1	A vulnerability exists in the configuration files because no authentication is required, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Oracle 9i Default Configuration File Information Disclosure	**Medium**	Bug discussed in newsgroups and websites. There is no exploit code required.
Oracle Corporation[72]	Multiple	Oracle9iAS Web Cache 2.0.0.0-2.0.0.3, Oracle9i 9.0, 9.1, Oracle8i 8.1.7, 8.1.7.1, Oracle 9i Application Server 1.0.2	A vulnerability exists because no authentication is required to access the administrative pages, which could let an unauthorized malicious user perform administrative functions.	Access can be restricted through configuration. Specify authorized user names or an Administrative Database Access Descriptor in the configuration file /Apache/modplsql/cfg/wdbsvr.app.	Oracle 9iAS Web Administration Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[66] Bugtraq, March 14, 2002.
[67] SecurityFocus, March 22, 2002.
[68] SecurityFocus, March 10, 2002.
[69] CERT Advisory, CA-2002-08, March 15, 2002.
[70] CERT Advisory, CA-2002-08, March 15, 2002.
[71] CERT Advisory, CA-2002-08, March 15, 2002.
[72] CERT Advisory, CA-2002-08, March 15, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
PHP[73]	Multiple	FirstPost PHP FirstPost 0.1	A Path Disclosure vulnerability exists when a request is made for a non-existent page, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FirstPost Path Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
PHPNet Toolpack [74]	Unix	PHPNetTool pack 0.1	Two vulnerabilities exist: a vulnerability exists because metacharacters are not adequately filtered, which could let a remote malicious user execute arbitrary commands; and a vulnerability exists because an absolute path is not used when searching for the traceroute program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHPNet Toolpack Input Validation	**High**	Bug discussed in newsgroups and websites. Metacharacter vulnerability can be exploited via a web browser.
PHPProjekt Develop-ment Team[75]	Unix	PHPProjekt 3.1, 3.1a	A vulnerability exists due to lack of permissions in the filemanager module, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.phprojekt.com/phprojekt.zip	PHPProjekt Permissions	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Qualcomm [76]	Windows 95/98/NT 4.0/2000	Eudora 5.1	A vulnerability exists when an e-mail is received that includes a file attachment because the file is automatically stored in a predictable location, which could let a remote malicious user execute arbitrary programs.	No workaround or patch available at time of publishing.	Eudora Known Attachment Location	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Qualcomm [77]	Unix	QPopper 4.0-4.03	A remote Denial of Service vulnerability exists when a string of approximately 2048 characters is sent.	No workaround or patch available at time of publishing.	QPopper Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
RSync[78]	Unix	RSync 2.4.1, 2.4.3, 2.4.4, 2.4.6, 2.5.0-2, 2.5.0-1, 2.5.1_1, 2.5.1, 2.5.2	A vulnerability exists because user privileges for supplementary groups are not properly dropped, which could let a malicious user obtain unauthorized access.	**RSync:** http://samba.anu.edu.au/rsync/download.html **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Slackware:** ftp://ftp.slackware.com/pub/slackware/	RSync Supplementary Group Privilege CVE Name: CAN-2002-0080	Medium	Bug discussed in newsgroups and websites.

[73] ALPER Research Labs Security Advisory, ARL02-A05, March 12, 2002.
[74] Bugtraq, March 18, 2002.
[75] Securiteam, March 16, 2002.
[76] SecurityFocus, March 18, 2002.
[77] Bugtraq, March 15, 2002.
[78] Mandrake Linux Security Update Advisory, MDKSA-2002:024, March 13, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Sun Micro Systems, Inc.[79]	Unix	Cobalt RaQ 2.0-4.0	A vulnerability exists in the 'MultiFileUpload.php' script, which could let a remote malicious user write arbitrary files on the system with root privileges.	No workaround or patch available at time of publishing.	Cobalt RaQ MultiFile Upload.php Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun Micro Systems, Inc.[80]	Unix	Solaris 7.0, 7.0_x86, 8.0, 8.0_x86	A vulnerability exists in the CGI script included with the CD because input is not properly sanitized, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Sunsolve CD CGI Script	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
SurfControl [81]	Windows NT 4.0/2000	SuperScout Email Filter SMTP 3.5.1	A Denial of Service vulnerability exists when a remote malicious user connects to the SMTP service and sends a 'HELO' or 'RCPT TO:' following by excessively long characters.	No workaround or patch available at time of publishing.	SurfControl Denial of Service	Low	Bug discussed in newsgroups and websites.
TalentSoft [82]	Windows 95/98/NT 4.0/2000, Unix	Web+ Server 4.6, 5.0	A buffer overflow vulnerability exists when a request is submitted for an unusually long .wml file, which could let a malicious user execute arbitrary code with SYSTEM privileges.	Patch available at: ftp://ftp.talentsoft.com/download/webplus/	Web+ Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Trend Micro, Inc.[83]	Windows NT 3.5/3.5.1/ 4.0, Unix	Interscan Viruswall (HP-UX) 3.6, (Linux) 3.6, (Solaris) 3.6, VirusWall for Windows NT 3.51	A vulnerability exists in the default configuration of the HTTP proxy when a malicious web server provides a modified HTTP header, which could let virus-infected content pass.	No workaround or patch available at time of publishing.	InterScan VirusWall Scan Circumvention	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
VBulletin[84]	Unix	VBulletin 2.0 rc 3, 2.0 rc 2, 2.2.0-2.2.4	A Cross-Site Scripting vulnerability exists because script code is not filtered from URL parameters, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	VBulletin Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
VBulletin[85]	Unix	VBulletin 2.2.0-2.2.2, 2.0 rc 2, 2.0 rc 3	A Cross-Site Scripting vulnerability exists because image tags are not adequately filtered, which could let a malicious user execute arbitrary script code.	Users may find details on how to obtain an upgrade at the following link: http://www.vbulletin.com/download/	VBulletin Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.

[79] Bugtraq, March 8, 2002.
[80] Bugtraq, March 11, 2002.
[81] Vuln-Dev, March 9, 2002.
[82] NGSSoftware Insight Security Research Advisory, NISR13032002, March 13, 2002.
[83] Inside Security GmbH Vulnerability Notification, March 10, 2002.
[84] SecurityFocus, March 21, 2002.
[85] Bugtraq, March 20, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Webmin[86]	Unix	Webmin 0.1-0.7, 0.8.3, 0.8.4, 0.21, 0.22, 0.31, 0.41, 0.42, 0.51, 0.76-0.80, 0.85, 0.88, 0.91, 0.92, 0.92-1	A vulnerability exists because script code is not properly filtered from output, which could let a malicious cause arbitrary code to be executed by the root user.	Upgrade available at: http://www.webmin.com/download/webmin-0.93.tar.gz	Webmin Script Code Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Webmin[87]	Unix	Webmin 0.92, 0.92-1	A vulnerability exists because the '/var/webmin' directory is created with world-readable permissions, which could let a malicious user hijack the session of the root user.	Upgrade available at: http://www.webmin.com/download/webmin-0.93.tar.gz	Webmin Directory Permissions	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Workforce ROI[88]	Multiple	Xpede 4.1, 7.0	Two vulnerabilities exist: a vulnerability exists because the username and password data is stored using a weak encryption method, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'Remember by password' option when a user tries to reauthenticate, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Xpede Password Exposure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published for the weak encryption vulnerability. There is no exploit code required for the reauthen-tication vulnerability.
Xerver[89]	Windows 95/98/NT 4.0/2000, XP	Xerver 2.10	Two vulnerabilities exist: a Denial of Service vulnerability exists when an excessive number of requests for 'C:\' is sent to port 32123; and a Directory Traversal vulnerability exists due to improper filtering, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.javascript.nu/xerver/	Xerver Denial of Service and Directory Traversal	Low/ Medium (Medium for the Directory Traversal vulner-ability)	Bug discussed in newsgroups and websites. The DoS exploit has been published. The Directory Traversal vulnerability can be exploited via a web browser.
Xqus[90]	Multiple	X-News 1.0, 1.1	A vulnerability exists due to insecure user database permissions, which could let an unauthorized malicious user obtain access to the administrative account.	No workaround or patch available at time of publishing.	X-News Insecure User Database Permissions	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[86] Securiteam, March 22, 2002.
[87] Securiteam, March 22, 2002.
[88] Bugtraq, March 22, 2002.
[89] Securiteam, March 8, 2002.
[90] SecurityFocus, March 13, 2002.

			Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name		Attacks/ Scripts
Xqus[91]	Multiple	X-Stat 2.2, 2.3	Multiple vulnerabilities exist: a Path Disclosure vulnerability exists when erroneous web requests are submitted, which could let a remote malicious user obtain sensitive information; an Information Disclosure vulnerability exists, which could let a remote malicious user obtain path information; and a Cross-Site Scripting vulnerability exists because arbitrary script are not properly filtered from URL parameters, which could let a remote malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	X-Stat Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. The Path and Information Disclosure vulnerabilities can be exploited via a web browser.
ZyXel[92]	Multiple	Zywall10 0.0V3.50 (WA.1), 0.0V3.24 (WA.2), (WA.1), (WA.0), 0.0V3.20 (WA.1), (WA.0)	A remote Denial of Service vulnerability exists when a malformed ARP packet with an invalid MAC address is sent to an interface on the system.	Upgrade available at: ftp://ftp.zyxel.com/download/public/firmware	Zywall10 Denial of Service	Low	Bug discussed in newsgroups and websites. This vulnerability can be exploited with numerous available tools.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

[91] SecurityFocus, March 13, 2002.
[92] Bugtraq, March 11, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 8 and March 22, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 15 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

March 22, 2002	Apache.win32.txt	Exploit URL's for the Apache Win32 Batch File Command vulnerability.
March 22, 2002	Nbtenum21.zip	A utility for Windows that can be used to enumerate NetBios information from one single host or an entire class C subnet. The information that is enumerated includes the account lockout threshold, local groups and users, global groups and users, and shares.
March 22, 2002	**Xdeep.pl**	**Perl script which exploits the Xpede Password Exposure vulnerability.**
March 19, 2002	Lcrzo-4.06-src.tgz	A toolbox for network administrators and malicious users that contains over 200 functionalities.
March 19, 2002	Onesixtyone-0.3.tar.gz	A SNMP scanner that utilizes a sweep technique to achieve good performance, finds SNMP devices on the network, and brute-forces the community strings using a dictionary.
March 19, 2002	Wellenreiter-V08.tar.gz	A GTK/Perl program that makes the discovery and the auditing of 802.11b wireless-networks much easier. It has an embedded statistics engine for the common parameters provided by the wireless drivers, enabling you to view details about the consistency and signal strength of the network. A scanner window can be used to discover access-points, networks, and ad-hoc cards.
March 14, 2002	**Debploit.zip**	**Exploit for the Windows 2000/NT 4.0 Privilege Elevation vulnerability.**
March 13, 2002	Ucd-Snmp.c	Exploit for the UCD-SNMP v4.2.1 Community String Overflow vulnerability.
March 12, 2002	**Ptrace-dark.c**	**Script which exploits the Penguin Traceroute Arbitrary Command Execution vulnerability.**
March 11, 2002	**Spherebreak.c**	**Script which exploits the SPHEREserver Denial of Service vulnerability.**
March 11, 2002	**Sscdsuncourier-ex.pl**	**Perl script which exploits the Sunsolve CD CGI Script vulnerability.**
March 9, 2002	**Citadel_Killer.c**	**Script which exploits the Citadel/UX Denial of Service vulnerability.**
March 9, 2002	**Smashxtux.pl**	**Perl script which exploits the XTux Server Denial of Service vulnerability.**
March 8, 2002	**LocaltTimerace-xtr.pl**	**Perl script which exploits the Cobalt RaQ MultiFile Upload.php Authentication Bypass vulnerability.**
March 8, 2002	**Symlink-time.sh**	**Exploit for the Cobalt RaQ MultiFile Upload.php Authentication Bypass vulnerability.**

Trends

- **Windows users should be suspicious of a new Internet worm that is disguised as a Microsoft security bulletin. The "W32/Gibe" worm masquerades as an "Internet Security Update" from Microsoft Corporation. For more information see Virus Section, W32/Gibe-A.**
- **The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner. For more information, see CERT® Incident Note IN-2002-03, located at: http://www.cert.org/incident_notes/IN-2002-03.html.**
- **The National Infrastructure Protection Center is aware of potential vulnerabilities existing within the Simple Network Management Protocol (SNMP) -- a protocol used by routers, switches and hubs on the Internet and other related equipment. For more information, see NIPC ALERT 02-001, located at: http://www.nipc.gov/warnings/alerts/2002/02-001.htm.**
- **The National Infrastructure Protection Center (NIPC) has received reporting that infrastructure related information, available on the Internet, is being accessed from sites around the world. While in and of itself this information is not significant, it highlights a potential vulnerability. For more information, see NIPC ADVISORY 02-001, located at: http://www.nipc.gov/warnings/advisories/2002/02-001.htm.**
- **The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in CA-2001-31 and discussed in VU#172583. For more information, see CERT® Advisory CA-2002-01, located at: http://www.cert.org/advisories/CA-2002-01.html.**
- **NIPC has updated their advisory, NIPC Advisory 01-030, regarding what Microsoft refers to as a critical vulnerability in the universal plug and play (UPnP) service in Windows. For more information see, NIPC ADVISORY 01-030.3, located at: www.nipc.gov/warnings/advisories/2001/01-030-2.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

	Common Name			
1	W32/SirCam.A	Worm	Stable	July 2001
2	W32/BadTrans.B	Worm	Stable	April 2001
3	W32/Klez.E	Worm	Increase	January 2002
4	W32/Nimda.A	File, Worm	Slight Decrease	September 2001
5	W32/Hybris.B	File, Worm	Stable	November 2000
6	W32/Magistr.B	File, Worm	Stable	March 2001
7	W32/Magistr.A	File, Worm	Stable	March 2001
8	Found.C	Worm	New to Table	March 2002
9	W32/MyParty.A	File, Worm	Decrease	January 2002
10	W32/Funlove.4099	File	Stable	November 1999

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **201** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **463** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Linux.Jac.8759 (Linux Virus): This is a virus that infects files under Linux. The virus infects ELF executables that exist in the same directory as the virus. When Linux.Jac.8759 is executed, it starts by checking all files that are in the same directory as the one from which the virus was executed. If it finds executable files that have write permission, it attempts to infect them. The virus will not infect files that end with the letters ps, nor will it infect files that were not created for the x86 (Intel) platform. The virus modifies several fields in the header of the file. One of the modifications is used as an infection marker. This check prevents the virus from infecting a file multiple times.

VBS/Doublet (Alias: VBS/Generic) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book. The worm arrives through e-mail in the following format:

- Subject: Re: <random characters.vbs> for you
- Body: Hi <recipient>, Look at this attached found on the net. See you soon
- Attachment: (same as file as subject line)

If executed, the worm copies itself in the \windows\ directory under the filename "doublet.vbs." Additionally, it will add the file "Doublet.sys" to the root directory on the hard drive. It will then search and infect all *.vbs files it finds. It makes the following modification:

- Lowers the Microsoft Word security levels

If the system date is equal to 10, VBS/Doublet displays the message box with the text, W97M/VBS.Doublet. Hahahahahaha....."

VBS/LoveLet-DO (Visual Basic Script Worm): This is a minor variant of VBS/LoveLet-AS Visual Basic Script virus. The worm forwards itself in an e-mail with the following characteristics:

- Subject line: US PRESIDENT AND FBI SECRETS =PLEASE VISIT =>(http://<website omitted>)<= or a random 6 letter string.
- Body text: VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRETPICTURE.. or a random 10 letter string.
- Attachment: random attachment name

On 17 September, the worm displays a message box containing the text, "Dedicated to my best brother=>Christiam Julian(C.J.G.S.) Att. TEGIF (M.H.M. Team)" where "TEGIF" can be any random 5 letters. VBS/Lovelet-DO attempts to download the files MACROMEDIA32.ZIP, LINUX321.ZIP and LINUX322.ZIP via Internet Explorer. Despite their filenames these files are not true ZIP files but rather a text file and two bitmap graphic files. MACROMEDIA32.ZIP is copied to the Windows directory with the

filename IMPORTANT_NOTE.TXT and set to run in the Registry. VBS/LoveLet-DO changes the Registry keys:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\=plan colombia,
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\=LINUX32\<systemdir>"\LINUX32.vbs"
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run=Services\reload\<windowsdir>\"reload.vbs"

so that the worm file runs on Windows startup. The two other files are copied to the Windows directory as LOGOS.SYS and LOGOW.SYS, respectively. The worm makes copies of itself (using the filenames LINUX32.VBS and RELOAD.VBS) and sets them to run at startup. It creates a copy of itself in the System directory with a filename of 5 to 8 characters with either the extension .GIF.VBS or .JPG.VBS. This is the file that is mailed out to all addresses in your Outlook address book.

W32.Alcarys.D@mm (Win32 Worm): This worm is similar to W32.Alcarys.C except that it also has the ability to spread using Microsoft Outlook.

W32Yaha.B@mm (Aliases: YAHA, YAHA.B, FRIENDS.SCR, W32/Valscr.A-mm) (Win32 Worm): This is a slight variant of W32.Yaha@mm. The difference between the two is in the files that the worm drops. Instead of C:\Recycled\Msscra.exe and C:\Recycled\Msmdm.exe, the worm drops two randomly named executables into the C:\Recycled folder.

W32/Caric-A (Aliases: W32.Caric@mm, W32/MyLife.b@MM) (Win32 Worm): This virus has been reported in the wild. It is a worm that arrives in an e-mail with the following characteristics:

- Subject line: bill caricature
- Attached file: cari.scr

If you run the attachment and Outlook is installed, then W32/Caric-A will send itself to the addresses in your address book. The worm also displays a cartoon of a man wearing a "Bill" badge and playing a saxophone. The worm saves a copy of itself in the Windows system folder and adds the following value to the registry:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\win = "C:\Windows\System\cari.scr"

W32/Chiton.b (Alias: W32/Gemi) (PE File Infector): This is slight variation of W32/Chiton.A, a PE (Portable Executable) File Infector that arrived as file "CHTHOM.EXE." It attempts to locate files with different PE file types to insert its viral code. The worm copies itself in the \%windows%\ directory under the filename "Gemini.exe."

W32/FBound-C (Aliases: W32/Impatt-a, WORM_JAPANIZE.A, W32/Impat) (Win32 Worm): This worm has been reported in the wild. It is an Internet worm that sends itself to everyone in your address book, using its own SMTP routines. The e-mail will have the following characteristics:

- Subject line: Important
- Attached file: Patch.exe

The message body of the e-mail will be blank. Please note: When the worm sends itself to an e-mail address ending in .jp (signifying Japan), the worm will use one of 16 different subject lines using Japanese characters. The worm does not have a destructive payload, does not change any Registry keys and does not drop any files. However, since there is a bug in the worm because it does not comply with SMTP encoding standards, it may sometimes bounce when it e-mails itself or may arrive in a non-working truncated form.

W32/Gibe-A (Alias: W32/Gibe@MM) (Win32 Worm): This worm has been reported in the wild. It is a worm that spreads attached to an e-mail, which appears to come from Microsoft. The e-mail will have the following characteristics:

- Subject line: Internet Security Update
- Attached file: q216309.exe

If q216309.exe is run it will display the message "This will install Microsoft Security Update. Do you wish to continue? ." It then copies itself to q216309.exe in the Windows folder and vtnmsccd.dll in the Windows system folder. It also drops and executes bctool.exe, winnetw.exe and gfxacc.exe in the Windows

folder and creates the file 02_n803.dat in which it stores information about e-mail recipients. Bctool.exe and winnetw.exe attempt to send out the e-mails as described above. Gfxacc.exe runs as a background process and opens port 12387, which could allow an intruder to gain remote access and control over the machine.
The worm sets the following registry keys:

- HKLM\Software\AVTech\Settings\Default Address = <default address>
- HKLM\Software\AVTech\Settings\DefaultServer = <default server>
- HKLM\Software\AVTech\Settings\Installed = ...by Begbie
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\3dfx Acc = <path to gfxacc.exe>
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\LoadDBackup = <path to bctool.exe>

W32/Porkis@MM (Aliases: I-Worm.Borzella, W32.Atram@mm, W32.Storiel@mm, WORM_PORKIS.A) (Win32 Worm): This mass-mailing worm contains its own SMTP engine, and is designed to use the system default SMTP server for spreading itself to addresses found in the Windows Address Book. The worm most likely originates from Italy. Once executed on the victim machine, the worm displays a series of message boxes (in Italian, progressing through a dialogue). The worm copies itself to the Windows directory as DLLMGR.EXE. This exe file is added to the registry so Windows will start the worm when the computer starts. The registry value is:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Dll manager

After this, it displays seven message boxes with Italian messages and exits. The installed copy at next startup opens the Windows Address Book and mails itself to all the addresses it can find there. Due to a bug in the code, the worm can't find the correct addresses in the WAB file so it is unable to spread.

W32/Shrew@MM (Alias: SHREW.A, WORM_SHREW.A) (Win32 Worm): This Internet worm, created in Visual Basic, uses Microsoft Outlook to propagate copies of itself via e-mail to the e-mail recipients listed on the infected user's Windows Address Book (WAB). The details of the e-mail that this worm arrives with are as follows:

- Subject:Try this, pretty cool
- Attachments:ActiveM.exe, List.txt

W97M.SMDM.A (Word 97 Macro Virus): This is a macro virus that only replicates to the Microsoft Word Normal.dot template. On the 5th of March, June, September, or December it will add instructions to the Autoexec.bat file to delete all files and folders on the C drive upon the next reboot.

WM97/WMVG-C (Word 97 Macro Virus): This is a macro virus created from the WMVG macro creation kit. The virus drops a VBScript to re-infect Word.

WORM_CERVIVEC.A (Aliases: CERVIVEC.A, W32.Cervivec.A@mm) (Internet Worm): This worm propagates by sending a copy of itself to all of the infected user's ICQ contacts. Its non-destructive payload displays worm-like lines in the screen of the infected system.

WORM_CHILLER.A (Alias: CHILLER.A) (Internet Worm): This worm, created in Visual Basic, uses Microsoft Outlook to email itself to all addresses listed in the infected user's address book. The details of the email it arrives with are as follows:

- Subject: 101 Reasons Why You Should Have Sex When You're Drunk
- Attachment: Reasons.exe

WORM_DENA.A (Alias: DENA.A) (Internet Worm): This mass-mailing worm sends itself to all recipients listed in the infected user's Microsoft Outlook address book. It arrives in an e-mail with details as follows:

- Subject: RE: I urgently need files for my computer
- Message Body: ….. really? Here are some useful files... enjoy...
- Attachments: modembooster.exe, keygen.com, chain.eml, mystique.scr, readme.pif

WORM_FINTAS.C (Aliases: FINTAS, FINTAS.C, I-Worm.Fintas) (Internet Worm): This high level worm, created in Visual Basic 6.0, arrives with the following characteristics:

- ? Message Body: the cool game about Final Fanstasy VIII :)
- ? Attachment: FF8.EXE

WORM_KLEZ.C (Aliases: W32/Klez.C@mm, W32.Klez.gen@mm, KLEZ.C, I-Worm.Klez.C) (Internet Worm): This destructive, persistent, memory resident, multi-process, and multi-threaded worm spreads a copy of itself via e-mail and Network shared drives. This worm consists of two components. The main worm and a Windows executable infector. Similar to PE_NIMDA.A, this worm also utilizes the exploits for MS Outlook and Outlook Express, which allow the automatic execution of an attachment during preview. On Windows NT/2K systems, this worm registers itself as a system service. On Windows 9X, it is hidden from the Task List.

WORM_KLEZ.D (Aliases: W32.Klez.D@mm, W32/Klez.d@MM) (Internet Worm): This worm propagates via e-mail and network shared drives. It is similar to WORM_KLEZ.A and the other variants in functionality. The e-mail it sends carries the file infector, PE_ELKERN.A, the same EXE file infector that WORM_KLEZ.A carries. On odd numbered system months (January, March, May, July, September, and November), it zeroes out all the files in the network shared drives.

Worm/Petik (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the infected users Address Book. If executed, the worm copies itself in the \windows\%system% directory under the filename "Flash32.exe." Additionally, it will add the file "FlashNet.htm" to the \windows\%system% directory. Each time a user restart their computer the following registry key gets added:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run=
Flash32=C:\WINDOWS\SYSTEM\Flash32.exe –I

It will also add the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\LiteLo

Worm/Yever (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects from the infected users Address Book. If executed, the worm copies itself in the \windows\%system% directory under the filename "nb32.exe." Each time a user restarts their computer, the following registry key gets added:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
nb32=C:\Windows\System\nb32.EXE

Worm/Yever contains the following text, "Yellow Fever BioCoded by GriYo /29A."

X97M.Gluas (Excel 97 MacroVirus): This is a macro virus that infects Microsoft Excel workbooks. It does not contain a destructive payload.

X97M.Laroux.UA (Excel 97 Macro Virus): This is an Microsoft Excel macro virus. It infects from an infected spreadsheet that it creates in the \XLstart folder. The infected sheet will be named either Teste.xls or Personal.xls.

XM97/Tris-A (Aliases: X97M_BREP.B, Macro.Excel97.Brep.b) (Excel 97 Macro Virus): This virus creates the viral file XLStart.xls in the XLStart directory. It has no malicious payload.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	**N/A**	**Current Issue**
BackDoor-ABN	**N/A**	**Current Issue**
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/Osiris:	**N/A**	**Current Issue**
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	**N/A**	**Current Issue**
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
SecHole.Trojan	N/A	CyberNotes-2002-01
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	**N/A**	**Current Issue**
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04

Trojan	Version	CyberNotes Issue #
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	**N/A**	**Current Issue**

BackDoor-ABH: This Remote Access Trojan masquerades as a downloader for an e-mail client application. When executed on the victim machine, the Trojan attempts to connect to an FTP server. The Trojan contains the string:

"Would you like to download Bmail.. Bmail is a talking E-mail software that works with POP and other e-mail accounts. Its works with Yahoo also. More will be added soon."

In addition to opening this FTP connection, the worm opens an additional port on the victim machine, enabling remote access to the machine. The Trojan sets the following Registry key in an attempt to run itself at system startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion_ Run "SetFTPBack" = C:\WINDOWS\SYSTEM\createsw.exe

BackDoor-ABN: When the server component of this Remote Access Trojan (dubbed 'AceBot' by its author) is executed on the victim machine, the Trojan copies itself to the Windows System directory as a randomly named executable, deleting the original file. The Trojan disables personal firewall in use. Strings within the Trojan suggest that the following personal firewalls will be bypassed:

- Sygate Personal Firewall
- Tiny Personal Firewall
- ZoneAlarm Pro
- ZoneAlarm

The Trojan sets the following Registry key to ensure it is executed at subsequent system startups (adjust the filename as necessary):

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion_ \Run "Microsoft Diagnostic" = C:\WINDOWS\SYSTEM\TJSTBU.EXE

Once running, the Trojan attempts to connect to an IRC server, in order to join a channel and listen for remote commands. Strings within the server suggest a variety of functions may be performed remotely. These include the following:

- Shutdown server (self kill)
- Issue channel message
- Sleep
- Update server
- Run file
- Download files
- Send packets
- Logoff machine
- Shutdown machine

Due to the wide variety of functions offered by this Remote Access Trojan, the payload danger is highly variable. Also, since this Trojan appears to be able to update itself, other functions may also be possible.

BDS/Osiris: This Trojan will allow someone with malicious intent backdoor access to your computer and allow them to perform various operations (ie. opening and closing the CD-ROM drive). If executed, the Trojan adds the following file to the \windows\%system% directory with hidden attributes, "kernel32.exe." So that it gets run each time a user restart their computer the following registry key gets added:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Kernel32=C:\WINDOWS\SYSTEM\kernel32.exe

BKDR_WARHOME.A (Aliases: TROJ_WARHOME.A, WARHOME.A, WARHOME, Backdoor.Komut, Troj/Komut): This backdoor Trojan has a server program and a client program. It uses the server program on target computers and the client program to access the target computers. The client side can delete files and folders on the target system running the server program. It compromises network security.

TROJ_JUNTADOR.B (Alias: JUNTADOR.B): This Trojan is compiled in Delphi, and is capable of sending ICQ messages. It drops files in the Windows directory and the System directory. It drops two backdoor programs, detected as BKDR_PSYCHWARD.F and BKDR_OBLIVION.B1.

W32.Delalot.B.Trojan: This is a Trojan horse that attempts to delete all files on all hard drives. If W32.Delalot.B.Trojan is executed, it first attempts to delete all files in all folders and subfolders on all hard drives. Then it drops the text file Piracy.txt into the root folder and displays a message.